

**AFFIDAVIT  
of  
SEAN McDERMOTT  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION**

I, Sean McDermott, being first duly sworn, do depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and am assigned to the Jefferson City, Missouri Office. I have been an SA with the FBI for approximately fifteen (15) years. In the course of my career, I have participated in numerous investigations concerning violations of Title 18, United States Code. I am currently assigned to criminal investigations involving child exploitation, child pornography and human trafficking. I have gained expertise in the conduct of such investigations through training in seminars and everyday work related to these types of investigations. I have personally led multiple investigations involving child exploitation, child pornography and human trafficking.

2. The statements contained in this affidavit are based on information I learned through my personal knowledge, investigative reports from other investigators familiar with this investigation, and conversations with investigators familiar with this investigation. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2422(b), specifically attempted coercion and enticement of a minor, and Title 18, United States Code 1591(a) and 1594, is present in the items to be searched.

3. I make this affidavit in support of search warrants for the following:

a. **19-3077-SW-WJE:** The residence located at 507 Copperhead Court, Columbia, Boone County, Missouri (the Residence); and

b. **19-3078-SW-WJE:** A white 2009 Mercury Milan, VIN 3MEHM08199R624833, with Missouri license plate number GE6-F3Z.

**PROBABLE CAUSE**

4. On July 29, 2019, a concerned citizen who wishes to remain anonymous (C.C.) was solicited by an individual who law enforcement subsequently identified as JEFFREY CHARLES JOHNSON, to find a juvenile female for a sexual encounter. JOHNSON texted C.C. from telephone number 573-303-6435 in response to a posting C.C. made on skipthegames.com, a dating website frequented by prostitutes advertising their services.

5. After discussing a rendezvous at C.C.'s residence, JOHNSON and C.C. had the following conversation:

JOHNSON: Will i do want to see you. Could you set me up with someone younger? Could pay you more also.

C.C.: I don't know anyone off top of head but I can try and contact some and get back with u I believe she is 19. What time would u like to meet?

JOHNSON: Like 5? And i mean younger than that.

C.C.: Are u talking about a minor?

JOHNSON: Yes.

C.C.: Because if u are I don't do that don't know any minors that do that and wouldn't help find a minor for that. I'm not the police or anything that's just not ok to do tho. How young are u talking?

JOHNSON: 12 13 14 but forget it. I will leave you alone.

6. After C.C. reported this conversation to the Boone County Sheriff's Department (BCSD), BCSD Detective Tracy Perkins orchestrated a ruse to assume the identity of a single mother, "Julie," willing to allow JOHNSON to have sex with her juvenile daughter. At Det. Perkins' direction, on July 30, 2019, C.C. referred JOHNSON to "Julie" via the following conversation:

C.C.: Hey I might have a friend that is interested in what your looking for.

JOHNSON: Do tell which part.?

C.C.: Sorry I was in shower. And about the minor part that you were interested in.

JOHNSON: Could you share more info?

C.C.: I spoke with a friend name Julie and she has a daughter...dont know much but you can talk to her.

JOHNSON: Ok i hope you arent setting me tp.

C.C.: No not at all I just know a girl that is single mom and she needs cash...just trying to take care of a friend in need that's all.

7. C.C. provided JOHNSON a telephone number for "Julie," and Det. Perkins subsequently began communicating with JOHNSON via text messages and telephone conversations. At JOHNSON's request, "Julie" sent two photographs of her daughter (in reality these photographs were of a BCSD employee), who she described as being 13 years old and called "Krissy." JOHNSON requested a "more seductive revealing picture" of "Krissy" in a bikini or in her bra and underwear.

8. On August 1, 2019, JOHNSON texted “Julie,” “Does krissy think im a creep for wanting to have sex with her?” and “Ok better question, do you think im a creep for wanting to have sex with krissy?”

9. On August 1, 2019, JOHNSON telephoned “Julie” at the telephone number provided to him by C.C. During this conversation, JOHNSON questioned “Krissy’s” sexual experience, reported this was on his bucket list, and offered to pay “Julie” a couple hundred dollars. “Julie” informed JOHNSON that “Krissy” was turning 14 years old in two months. JOHNSON reported he lived in north Columbia at the back of Vanderveen subdivision. (Note: JOHNSON used the alias “Mike” during this and subsequent telephonic conversations with “Julie.”)

10. On August 5, 2019, JOHNSON telephoned “Julie” at the telephone number provided to him by C.C. JOHNSON and “Julie” arranged for JOHNSON to meet her and “Krissy” at the Red Roof Inn in Columbia, Missouri, on August 7, 2019, at approximately 12:40 p.m. JOHNSON advised he would have cash on hand for “Julie” before they walked up to the hotel room.

11. On August 6, 2019, JOHNSON telephoned “Julie” at the telephone number provided to him by C.C. JOHNSON discussed his intention to engage in sexual acts with “Krissy” when they met at the Red Roof Inn. JOHNSON reported he would bring condoms to their rendezvous.

12. On August 7, 2019, JOHNSON telephoned “Julie” at the telephone number provided to him by the CC. JOHNSON and “Julie” discussed “Krissy” giving him oral sex. Acting in an undercover capacity as “Krissy,” BCSD Deputy Laurel Martin then spoke to JOHNSON. JOHNSON and “Krissy” discussed her giving him oral sex. JOHNSON questioned if Krissy had sexual experience with older men, and told her he would like to “experience everything.”

13. At approximately 11:23 a.m. on August 7, 2019, law enforcement officers observed JOHNSON's 2009 white Mercury Milan bearing Missouri license plate GE6-F3Z departing his workplace at 1801 Commerce Court, Columbia, Missouri. JOHNSON drove to a gas station across from the Red Roof Inn, stopped briefly, then drove to the motel. JOHNSON met with "Julie" in the hotel parking lot, then drove his car to the rear side of the motel where he expected to meet "Krissy." Upon parking his car, JOHNSON was arrested by BCSD deputies, who found a wrapped condom in JOHNSON's jeans pocket.

14. JOHNSON was transported to the BCSD. After being read his *Miranda* warnings and agreeing to speak to BCSD Det. Andy Evans, JOHNSON confirmed his identity and address of 507 Copperhead Court, Columbia, Missouri. JOHNSON told Det. Evans that he was referred to "Julie" by a prostitute he had met on the Internet website skipthegames.com after inquiring about her finding an underage female for a sexual rendezvous. JOHNSON admitted he had conversed with "Julie" over approximately the next week for the purpose of setting up a sexual rendezvous with "Julie's" 13-year-old daughter, "Krissy." JOHNSON admitted he traveled to the Red Roof Inn to have oral sex, and possibly sexual intercourse, with "Krissy."

15. The Missouri Information Analysis Center reported telephone number 573-303-6435 was a Verizon Wireless telephone number assigned to JEFFREY C. JOHNSON of Columbia, Missouri. The Missouri Department of Motor Vehicles reported a 2009 Mercury Milan, VIN 3MEHM08199R624833, with Missouri license plate number GE6-F3Z, was titled in the name of JEFFREY C. JOHNSON, 507 Copperhead Court, Columbia, Missouri.

16. Public records from the Boone County Assessor's Office reported 507 Copperhead Court, Columbia, Missouri, was owned by JEFFREY C. JOHNSON and Rebecca C. Scott. On August 5, 2019, Det. Perkins observed a white Toyota Sienna bearing Missouri license plate CT0-

W5J parked in the driveway of 507 Copperhead Road. The Missouri Department of Motor Vehicles reported this vehicle was registered to Rebecca C. Scott.

### **Definitions**

17. I am aware that computer hardware and computer software may be utilized to store records which include, but are not limited to, those related to business activities, criminal activities, associate names and addresses, and the identity and location of assets illegally gained through criminal activity.

18. The terms "records," "documents" and "materials" include all information recorded in any form, visual or aural, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, returns, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets; and

b. Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes, and aural records or representations, tapes, records, disks.

19. The terms "records," "documents" and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications that may have been created or stored, including (but not limited to): any hand-made form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); and any electrical, electronic, or magnetic form (such as tape recordings,

cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, smart phones, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

### **Use of Computers With Child Exploitation**

20. The development of computers and smart phones has added to the methods individuals use to interact with and sexually exploit children. Computers serve four functions in connection with child exploitation cases, which are production of images, communication, distribution of images, and storage of images and communications.

21. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, smart phone, or mobile device, so that the image file is stored in his computer, phone, or mobile device.

22. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are

automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

23. The computer's capability to store images in digital form makes it an ideal repository for pornography. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera or camera on a phone to capture an image, process that image in a computer with a video capture board, and to save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

24. Smart phone technology, has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, produce photographic images, and store and view movie and picture files. Further, smart phone technology allows users to back the contents of their phone up to a computer and transfer image files from their smart phone to a computer or other electronic device.

## **The Internet and Technical Terms Pertaining to Computers**

25. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail (“e-mail”). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an “Internet Service Provider” or “ISP” (see definition of “Internet Service Provider” below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see definition of “websites” below), and make purchases from them.

26. Set forth below are some definitions of technical terms, used throughout this Affidavit pertaining to the Internet and computers more generally:

a. Computer system and related peripherals, and computer media: As used in this affidavit, the terms “computer system and related peripherals, and computer media” refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, smart phones, mobile devices in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including,

but not limited to, JPG, GIF, TIF, AVI and MPEG;

b. Internet Service Providers (ISPs) and the Storage of ISP Records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as “electronic storage,” see 18 U.S.C. § 2510(17), and the provider of such a service is an “electronic communications service.” An “electronic communications service,” as defined by statute, is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a “remote computing service.” 18 U.S.C. § 2711(2); and

c. Log File: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log on/logoff times and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

### **Specifics of Search and Seizure of Computer System**

27. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

28. Based upon my consultation with experts in computer searches, data retrieval from computers, and related media and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation,

and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

- a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable time;
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval;
- c. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of transmitting child pornography in violation of law, and should all be seized as such; and
- d. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the Residence are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

#### **Method of Searching and Examining Computers and Digital Evidence**

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone:* A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device;

b. *IP Address:* An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses; and

c. *Internet:* The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience and research, I know that computers and smart phones have capabilities that allow it to serve as a device to facilitate communications via the Internet, and also retain files containing contraband, and other related documents and communications, including email communications. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

31. Based on my knowledge, training and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes

be recovered with forensics tools.

32. There is probable cause to believe that things that were once stored on the computer(s) and smart phone(s) may still be stored there, for at least the following reasons:

a. Based on my knowledge, training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

33. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

34. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence

of the crimes described on the warrant, but also forensic evidence that establishes how the computer(s) and smart phone(s) were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the items because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created;
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence;
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when; and
- d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

36. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

### **Conclusion**

38. In view of the foregoing, there is probable cause to conclude that, in the areas to be searched, further described in Attachment A, there will be located evidence of a crime, contraband or the fruit or instrumentalities of a crime, of one or more violations of Title 18, United States Code, Section 2422(b) and Title 18, United States Code, Section 1591(a) and 1594. Accordingly, I respectfully request the issuance of a warrant to search the areas more fully described in Attachment A for the items described on Attachment B.

39. The facts set forth in this affidavit are true and correct to the best of my knowledge and belief.

Further, Affiant sayeth not.



---

**Sean McDermott**, Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me on this, the 7th day of August, 2019.



---

**Willie J. Epps, Jr.**  
United States Magistrate Judge